IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 3 (Jul. - Aug. 2013), PP 30-35
www.iosrjournals.org

Enhancement of Data Hiding Capacity in Audio Steganography

Sheelu[1]
[1](M. Tech (CSE) - Manav Rachna College Of Engineering, Faridabad, India)

Abstract: *Nowadays, a lot of applications are Internet-based and demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So a technique for secure transmission of messages called Steganography, which send the messages in such a way that existence of the message is concealed. Audio Steganography is the scheme of hiding the existence of secret information by concealing it into an audio file. In this paper we will discuss how audio file can be used as carrier to hide the secret information. In this paper we also proposed a system that will enhance the data hiding capacity in Audio Steganography using LSB method. we will use last 4 LSB's instead of a single LSB , this will enhance the data hiding capacity of carrier file.*

Keywords: *Steganography, Audio Steganography , Cover file, Stego file, key*

I. Introduction

Steganography[1] is the technique of hiding secret information in a communication channel in such a manner that the very existence of information is concealed. It is the science of "invisible" communication and prevents an unintended recipient from suspecting that the data exists. Steganography is derived from the Greek word steganos which means "Covered" and graphy means "Writing", i.e. covered writing. Many different carrier file formats can be used like Text, Images, and videos, but digital Images and Audios are the most popular because of their frequency on the Internet.

The Steganography hides different types of data within a cover file. The resulting stego file also contains hidden information, although it is virtually identical to the cover file. Steganography exploit human perception; human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography). The main goal of Steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data . It is not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a Steganography method causes someone to suspect there is a secret information in a carrier medium, then the method has failed

II. Different File Formats Used as Carrier in Steganography:

The four main categories of file formats[2] that can be used as carrier in Steganography are:
I. Text
II. Images
III. Audio/ Video
IV. Protocol

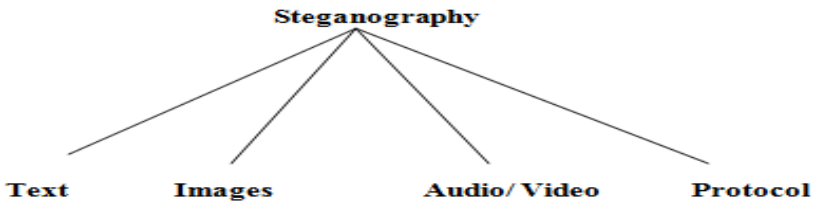

Figure 1:Different carriers in Steganography

I. **Text Steganography**: Hiding information in text is the most important method of Steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data

.

II. **Image Steganography:** Images are used as the popular cover objects for Steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

III. **Audio Steganography:** Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.

IV. **Protocol Steganography:** The term protocol Steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

III. Audio Steganography

Audio Steganography[3] is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. Thus embedding secret messages into digital sound is known as audio Steganography. Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files. The properties of the human auditory system (HAS) are exploited in the process of audio Steganography. Auditory perception is based on the critical band analysis in the inner ear where a frequency-to-location transformation takes place along the basilar membrane. The power spectra of the received sounds are not represented on a linear frequency scale but on limited frequency bands called critical bands

3.1 Digital Audio

Digital audio[3] is discrete rather than continuous signal as found in analog audio. A discrete signal is created by sampling a continuous analog signal at a specified rate. For example, the standard sampling rate for CD digital audio is about 44 kHz.

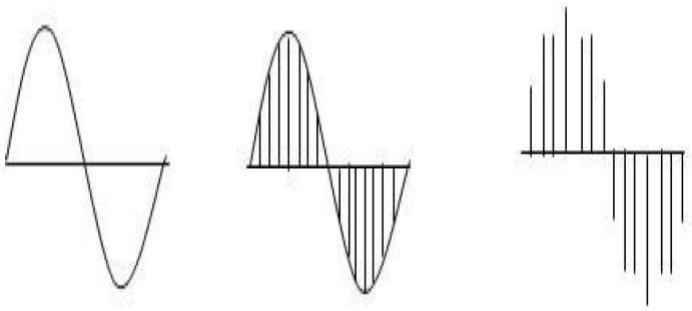

Figure 2: Continuous analog sound wave is sampled to produce digital signal

Digital audio is stored in a computer as a sequence of 0's and 1's. With the right tools, it is possible to change the individual bits that make up a digital audio file. Such precise control allows changes to be made to the binary sequence that are not discernible to the human ear. In the digital domain, PCM (Pulse Code Modulation) is the most straightforward mechanism to store audio. The analog audio is sampled in accordance with the Nyquest theorem and the individual samples are stored sequentially in binary format. The wave file is the most common format for storing PCM data and the WAVE file format is a subset of Microsoft's RIFF specification for the storage of multimedia files. That's why .wav files have been used here for below mentioned experiments

3.2. The basic model of Audio Steganography

The basic model of Audio Steganography[4] consists of Carrier (Audio file), Message, Password, Stego file. Carrier is also known as a cover-file, which conceals the secret information. Basically, the model for Steganography is shown in Fig 3. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file. Fig.3 shows the block diagram of a secure steganographic system. Input messages can be images, texts, video, etc. The components of steganographic system are:

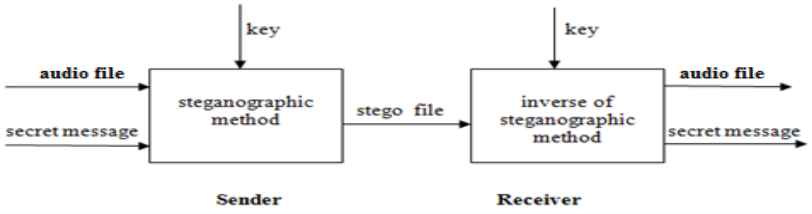

Figure 3. A generic Steganography System

secret message: The secret message or information to hide.
audio file: An audio file which concealed the secret message.
stego file: A modified version of audio file that contains the secret message.
key: Additional secret data that is needed for the embedding and extracting processes and must be known to both, the sender and the recipient
steganographic method: A steganographic function that takes audio file, secret message and key as parameters and produces stego as output.
inverse of steganographic method: A steganographic function that has stego and key as parameters and produces secret message as output. This is the inverse of method used in embeding process in the sense that the result of the extracting process is identical to the input of the embedding process.

The embedding process embeds the secret message in the audio file. The result of the embedding function is slightly modified version of audio file: the stego file. After the recipient has received stego file, he starts the extracting process with the stego file and the key as parameters. If the key that is supplied by the recipient is the same as the key used by the sender to embed the secret message and if the stego data the recipient uses as input is the same data the sender has produces, then the extracting function will produce the original secret message.

IV. Least Significant Bit (LSB) Encoding:

Least significant bit (LSB)[4] coding is the simplest way to embed information in a digital audio file, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz.

To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples.

1	0	0	1	0	1	0	1

Figure 4 : Binary representation of decimal 149

The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary number represents a value of 128 decimal. The LSB represents a value of 1. For example, to hide the letter "a" (ASCII code 97, which is 01100001) inside eight bytes of a cover, you can set the LSB of each byte like this:

10010010
01010011
10011011
11010010
10001010
00000010
01110010
00101011

Fig 5 illustrates how the message 'HEY' is encoded using the LSB method. Here the secret information is 'HEY' and the cover file is audio file. HEY is to be embedded inside the audio file. First the secret information 'HEY' and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of sectet information 'HEY'. The resulting file after embedding secret information 'HEY' is called Stego-file.

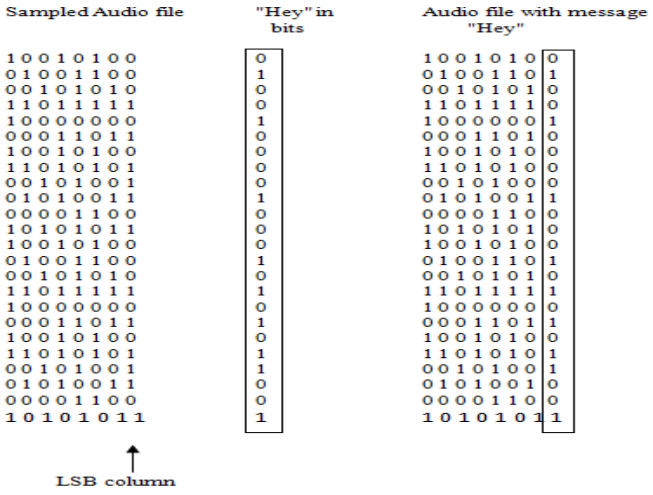

Figure 5 . LSB coding example

There are two main disadvantages associated with the use of methods like LSB coding. The human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file, Second disadvantage however, is that this is not robust. If a sound file embedded with a secret message using either LSB coding was resample, the embedded information would be lost. Robustness can be improved somewhat by using a redundancy technique while encoding the secret message. However, redundancy techniques reduce data transmission rate significantly.

V. Proposed system

In the proposed system, I will use last 4 LSB's instead of single LSB. By this we can store more bits of secret information in the single byte of carrier file. This will enhance the capacity of carrier file to conceal the secret information as shown in the figure.

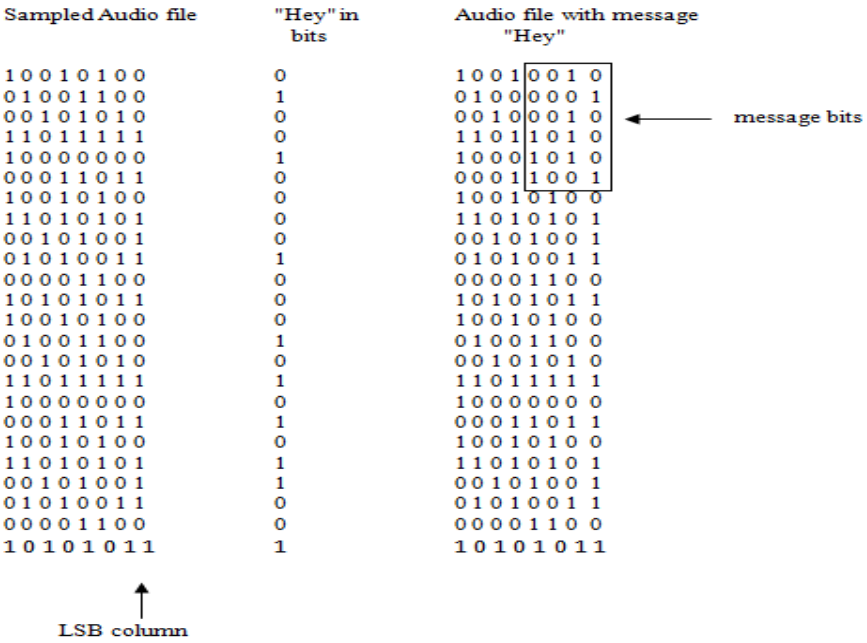

Figure 5 . Proposed system example

The Proposed system: The Proposed system is consist of following two phases
a) Sender side(Encoding process)
b) Receiver side(Decoding process)

5.1 Encoding Process on Sender Side (Secret Data Hiding)

Encoding process takes place at the sender side to hide the secret information. Here the carrier audio file and secret information will be converted into bits and then bits of secret information will hideen in the last 4 LSB's of carrier audio file. The steps of encoding process are as follows:

1. Convert the audio file to binary format.
2. Hide the secret information into an audio or carrier file.
3. Remove noise from the stego file by using the filter.
4. Generate the key using the stego and the filtered file.
5. Key and the filtered file are send to the receiver.

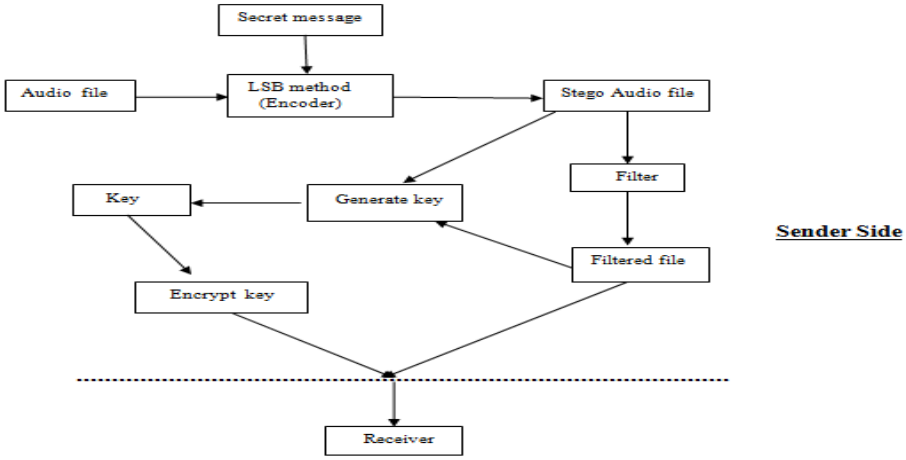

Figure 7 . Process on sender side in the proposed system

5.2 Decoding Process on Receiver Side (Secret Data Extraction)

Decoding process will takes place at the receiver side to extract the secret information. Here the key and filtered file are used to get the secret information. The steps of decoding process are as follows:

1. The receiver will decrypt the key .
2. The receiver will use the key to extract the stego file from the filtered file.
3. Receiver can extract the secret information from the extracted stego file.

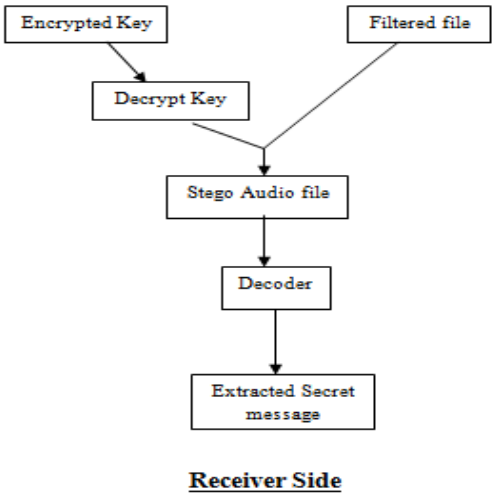

Figure 8 . Process on receiver side in the proposed system

VI. Conclusion

Steganography not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a Steganography method causes someone to suspect there is a secret information in a carrier medium, then the method has failed. Different file formats can be used as carrier in Steganography. Embedding secret information in an audio file is usually a more difficult process than embedding messages in other media. Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files. As we will hide 4 bits of secret information in each byte of the carrier. This will enhance the capacity of carrier and carrier will conceal a large amount of secret information. By this we can send a large amount of secret information in a audio file

References

[1] Jammi Ashok, Y. Raju, S. Munishankaraiah, K. Srinivas " Steganography : An Overview" in International Journal of Engineering Science and Technology Vol. 2(10), 2010, 5985-5992

[2] Pratap Chandra Mandal Modern "Steganographic technique: A survey" in International Journal of Computer Science & Engineering Technology (IJCSET)

[3] Prof. Samir Kumar Bandyopadhyay and Barnali Gupta "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited" in International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012

[4] Jayaram P, Ranganatha H R, Anupama H S, " Information Hiding Using Audio Steganography – A Survey" in The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011